Definition 1. A non-empty set G with a binary composition is called a *group* if the composition is associative, if a unique *identity* exists for all elements in G, and if a unique *inverse* exists for each of the elements in G. The group G is called *Abelian* if the composition in it is commutative for any two elements in G. A non-empty set R with two binary compositions, call these addition and multiplication, defined on it is called a *ring* if R is an Abelian group with respect to the composition addition, if multiplication in R is associative, and if distributive laws hold for all elements in R. A set F having at least two elements with two compositions, be them called addition and multiplication, defined on it is called a *field* if it is a commutative ring with identity every non-zero element of which has an inverse with respect to multiplication. A field having only a finite number of elements is called a *finite* or *Galois field.*

Example 1. The set

$$F_p = \{0, \ldots, p-1\}$$

in which addition and multiplication are defined modulo p, where p is a prime integer, is a finite field. For $p = 2$ we have $F_2 = \{0, 1\}$, which is denoted by $\mathbf{B}$. The set $\mathbf{B}^n$ of all ordered n-tuples or sequences of length n, a positive integer, with each tuple or entry of the sequence being in the field $\mathbf{B}$ and a composition defined as a componentwise summation of any two sequences in $\mathbf{B}^n$, is an Abelian group. The zero sequence of length n is the identity of $\mathbf{B}^n$ and each element in $\mathbf{B}^n$ is its own inverse.

Definition 2. A *binary block* (b,n)*-code* comprises an *encoding function*

$$E : \mathbf{B}^b \to \mathbf{B}^n$$

and a *decoding function*

$$D : \mathbf{B}^n \to \mathbf{B}^b$$

The images of E are called *code words*.

Definition 3. Let two binary sequences be a and b in $\mathbf{B}^n$. The *distance* $d(a, b)$ between a and b is defined as

$$d(a, b) = \sum_{i=1}^{n} x_i$$

where

$$x_i = \begin{cases} 0 & \text{if } a_i = b_i \\ 1 & \text{if } a_i \neq b_i \end{cases}$$

Definition 4. The *weight* $w(a)$ of a in $\mathbf{B}^n$ is the number of non-zero components of the sequence a.

Theorem 1. Let a and b be any two sequences in $\mathbf{B}^n$. Then $d(a,b) = w(a+b)$.

Proof. The only contribution of 1 to $d(a,b)$ is $a_i \neq b_i$ for all $1 \leq i \leq n$. But this latter is the case if and only if $a_i + b_i = 1$, and this contributes 1 to $w(a+b)$. ¶

Definition 5. Let X and Y be two groups. Then a map

$$f : X \to Y$$

which satisfies the property

$$f(x_1x_2) = f(x_1)f(x_2)$$

for all x_1 and x_2 in X is called a *homomorphism*. Further, the homomorphism f is called a *monomorphism* if it is one to one, and it is called an *isomorphism* if it is both one to one and onto.

Definition 6. A block code is called a *group code* if all its code words form an additive group.

Definition 7. A $b \times n$ matrix G over $\mathbf{B}$, where $b < n$, is called an *encoding-* or *generator matrix* if G is of the form

$$G = [I_b \, G_n]$$

where I_b is an identity matrix of dimension b and G_n a $b \times (n - b)$ matrix. An *encoding function* $E : \mathbf{B}^b \to \mathbf{B}^n$ is defined by

$$E(x) = xG$$

for all x in $\mathbf{B}^b$

Theorem 2. The encoding function $E : \mathbf{B}^b \to \mathbf{B}^n$ given by $E(x) = xG$ for all x in $\mathbf{B}^b$, where G is a $b \times n$ generator matrix, is a monomorphism.

Proof. Both $\mathbf{B}^b$ and $\mathbf{B}^n$ are additive Abelian groups. Then for all x and y in $\mathbf{B}^b$ we know that $x + y$ is also in $\mathbf{B}^b$ and

$$E(x+y) = (x+y)G = xG + yG = E(x) + E(y)$$

Thus E is a homomorphism. Further, as the first part of G is I_b, it follows that a part of $E(x)$ is x itself. Therefore the matrix encoding method gives for each binary message word a distinct code word. In other words, the mapping E is one to one, which means that it is a monomorphism. ¶

Definition 16. A code generated by a generating matrix is called a *matrix code.*

Theorem 3. A matrix code is a group code.

Proof. The code words generated by E are associative, since

$$x_1G + (x_2G + x_3G) = (x_1G + x_2G) + x_3G$$

They have a unique identity, that is the zero $b \times n$ matrix, and each of them is its own inverse. ¶

Definition 9. An $(b, b+1)$ parity check code is the code generated by an encoding function $E : \mathbf{B}^b \to \mathbf{B}^{b+1}$ defined by

$$E(a_1 \cdots a_b) = a_1 \cdots a_b a_{b+1}$$

where

$$a_{b+1} = \begin{cases} 1 & \text{if } w(a) \text{ is odd} \\ 0 & \text{if } w(a) \text{ is even} \end{cases}$$

$w(a)$ being $w(a_1 \cdots a_b)$.

Theorem 4. The $(b, b+1)$ parity check code is a group code.

Proof. Let our unencoded binary words be $a = a_1 \cdots a_b$, $b = b_1 \cdots b_b$, and $c = c_1 \cdots c_b$ such that $c_i = a_i + b_i$ for $i = 1, \ldots, b$, and let the coded words of a and b be respectively $\bar{a} = aa_{b+1}$ and $\bar{b} = bb_{b+1}$. Since c is odd if and only if either a is odd while b is even or vice versa, but when this is the case we have either $a_{b+1} = 1$ and $b_{b+1} = 0$, or $a_{b+1} = 0$ and $b_{b+1} = 1$. Either way we have

$$c_{b+1} = 1 = a_{b+1} + b_{b+1}$$

Next, c is even if and only if a and b are either both odd or both even. But when either of these is the case, then

$$a_{b+1} + b_{b+1} = 0 = c_{b+1}$$

Hence $\bar{c}$ is a parity-check code word. The zero word is the identity and the inverse of each word is that word itself. Therefore the set of all code words forms a group. ¶

Theorem 5. The minimum distance of a group code equals the minimum of the weights of its non-zero code words.

Proof. Let d_m be the minimum distance of the group code, and w_m the minimum of the weights of the non-zero code words of the same. Then there exist code words a and b such that

$$d_m = d(a, b) = w(a + b) \geq w_m$$

Now, w_m implies that there exists a non-zero code word c such that

$$w_m = w(c) = d(c, 0) \geq d_m$$

Hence $d_m = w_m$. ¶

Example 2. Let the generator matrix be

$$G = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}$$

The dimension of G is $b \times n$, which in this case is 3×6. Let $a_1a_2a_3a_4a_5a_6$ be the code word and $a_1a_2a_3$ the original word, then

$$(a_1\, a_2\, a_3\, a_4\, a_5\, a_6) = (a_1\, a_2\, a_3)\, G$$

and then,

$$\begin{aligned} a_4 &= a_1 + a_2 \\ a_5 &= a_1 + a_3 \\ a_6 &= a_1 + a_2 + a_3 \end{aligned}$$

In other words,

$$\left.\begin{aligned} a_1 + a_2 + a_4 &= 0 \\ a_1 + a_3 + a_5 &= 0 \\ a_1 + a_2 + a_3 + a_6 &= 0 \end{aligned}\right\}\text{parity check equations}$$

These parity check equations are then, in matrix form,

$$\begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} a_1 \\ a_2 \\ a_3 \\ a_4 \\ a_5 \\ a_6 \end{pmatrix} = 0$$

The matrix

$$H = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}$$

is called the *parity check matrix* of the code. Then $G = \begin{pmatrix} I_3 & A \end{pmatrix}$ and $H = \begin{pmatrix} A' & I_3 \end{pmatrix}$, where

$$A = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}$$

and

$$A' = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 1 \end{pmatrix}$$

Example 3. The parity check code in Definition 9 is in fact a matrix code given by the generator matrix

$$G = \begin{pmatrix} 1 & 0 & \cdots & 0 & 1 \\ 0 & 1 & & 0 & 1 \\ \vdots & & \ddots & & \vdots \\ 0 & & \cdots & 1 & 1 \end{pmatrix}$$

whose parity check matrix is the $1 \times (b+1)$ matrix $H = \begin{pmatrix} 1 & \cdots & 1 \end{pmatrix}$.

Definition 10. The *syndrome* of a word $r \in \mathbf{B}^n$ is

$$\mathbf{s} = H\mathbf{r}'$$

Algorithm 1 *the syndrome decoding algorithm.*

```
$r \leftarrow r_1 \cdots r_b r_{b+1} \cdots r_n$
$\mathbf{s} \leftarrow H\mathbf{r}'$
if $\mathbf{s} = 0$ then
    $b_r \leftarrow (r_1 \cdots r_b)$
elseif $\mathbf{s}$ matches the $i^{\text{th}}$ column of $H$ then
    $c_r \leftarrow (r_1 \cdots r_{i-1}(r_i + 1)r_{i+1} \cdots r_n)$
    $b_r \leftarrow (c_{r1} \cdots c_{rb})$
else
    at least two errors have occurred in the transmission
endif
```

Theorem 6. An $(n-b)\times b$ parity check matrix H will decode all single errors correctly if and only if the columns of H are distinct and non-zero.

Proof. Suppose the i^{th} column of H is zero, and let e be a word whose weight is 1 having 1 in the i^{th} position and 0 elsewhere. Then for any code word b, we have

$$H(\mathbf{b}+\mathbf{e})' = H\mathbf{b}' + H\mathbf{e}' = 0$$

So our decoding procedure becomes $D(b+e) = b+e$ and the error vector $\mathbf{e}$ goes undetected.

Next, suppose that the i^{th} and the j^{th} columns of H are identical. Let e^i and e^j be words of length n with 1 in the i^{th} and respectively j^{th} position and 0 elsewhere. Then for any code word b, we have

$$H(\mathbf{b}+\mathbf{e}^i)' = H\mathbf{b}' + H\left(\mathbf{e}^i\right)' = H\left(\mathbf{e}^i\right)' = H\mathbf{b}' + H\left(\mathbf{e}^j\right)' = H\left(\mathbf{b}+\mathbf{e}^j\right)'$$

We are unable to decide whether the error occurred in the i^{th} or the j^{th} position. Conversely, suppose all the columns of H are distinct and non-zero. Then for any code word b and any error vector $\mathbf{e}$ of weight 1 having 1 in the i^{th} position,

$$H\left(\mathbf{b}+\mathbf{e}\right)' = H\left(\mathbf{b}'+\mathbf{e}'\right) = H\mathbf{b}' + H\mathbf{e}' = 0 + H\mathbf{e}'$$

Our decoding procedure gives $D(b+e) = b$, therefore every single error is corrected. ¶

Theorem 7. If

$$G = \begin{pmatrix} I_b & A \end{pmatrix}$$

is a $b \times n$ generator matrix of a code, then

$$H = \begin{pmatrix} A' & I_{n-b} \end{pmatrix}$$

is the unique parity check matrix for the same code. If

$$H = \begin{pmatrix} B & I_{n-b} \end{pmatrix}$$

is an $(n - b) \times n$ parity check matrix, then

$$G = \begin{pmatrix} I_m & B' \end{pmatrix}$$

is the unique generator matrix for the same code.

Proof. Let the original word be $a \in \mathbf{B}^b$ and c be the code word corresponding to a with respect to the code given by the generator matrix G. Then $\mathbf{c} = \mathbf{a}G$ Let a be $a_1 \cdots a_b$. Since the first b columns of G is an identity matrix, it follows from $\mathbf{c} = \mathbf{a}G$ that $a_i = b_i$ for all $1 \leq i \leq b$. Let $\bar{c} = c_{b+1} \cdots c_n$, then $c = c_1 \cdots c_b c_{b+1} \cdots c_n$ and $\mathbf{c} = (\,\mathbf{a} \quad \bar{\mathbf{c}}\,)$. Then,

$$\begin{aligned} H\mathbf{c}' &= (\,A' \quad I_{n-b}\,)\,(\,\mathbf{a}G\,)' \\ &= (\,A' \quad I_{n-b}\,)\,G'\mathbf{a}' \\ &= (\,A' \quad I_{n-b}\,)\,(\,I_m A\,)'\,\mathbf{a}' \\ &= (\,A' \quad I_{n-b}\,)\begin{pmatrix} I_m \\ A' \end{pmatrix}\mathbf{a}' \\ &= (\,A'I_m + I_{n-b}A'\,)\,\mathbf{a}' \\ &= (\,A' + A'\,)\,\mathbf{a}' \\ &= 0 \times \mathbf{a}' \\ &= 0 \end{aligned}$$

Therefore c is the code word corresponding to the original word a in the code given by the parity check matrix H.

Now, suppose first that c is the code word corresponding to the original word a as above in the code obtained from the parity check matrix $H = \begin{pmatrix} A' & I_{n-b} \end{pmatrix}$. Then $c_i = a_i$ for all $1 \le i \le b$ and $H\mathbf{c}' = 0$. Let $\bar{c} = c_{b+1} \cdots c_n$. Then,

$$\begin{aligned} H \begin{pmatrix} \mathbf{a} \\ \bar{\mathbf{c}}' \end{pmatrix} &= 0 \\ \begin{pmatrix} A' & I_{n-b} \end{pmatrix} \begin{pmatrix} \mathbf{a} \\ \bar{\mathbf{c}}' \end{pmatrix} &= 0 \\ A'\mathbf{a}' + I_{n-b}\bar{\mathbf{c}}' &= 0 \end{aligned}$$

Therefore $\bar{c} = \mathbf{a}A$, and

$$\mathbf{c} = \begin{pmatrix} \mathbf{a} & \bar{c} \end{pmatrix} = \begin{pmatrix} \mathbf{a}I_m & \mathbf{a}A \end{pmatrix} = \mathbf{a}\begin{pmatrix} I_m & A \end{pmatrix} = \mathbf{a}G$$

Hence c is the code word corresponding to the original word a in the code defined by the generator matrix G. So far we have proved that codes determined by G and H are identical.

Suppose that to $G = (\, I_m \quad A\,)$ corresponds another parity check matrix $H_1 = (\, B \quad I_{n-b}\,)$. Let e^i be the original word with 1 in the i^{th} position and 0 elsewhere. The corresponding code word is $\mathbf{e}^i G$, that is the i^{th} row of G, or we may write $\mathbf{e}^i G = (\, \mathbf{e}^i \quad \tilde{\mathbf{e}}^i\,)$, where $\tilde{\mathbf{e}}^i$ is the i^{th} row of A. Since H_1 is a parity check matrix of the code defined by G, it follows that,

$$\begin{aligned} H_1 \,(\, \mathbf{e}^i \quad \tilde{\mathbf{e}}^i\,)' &= 0 \\ (\, B \quad I_{n-b}\,) \begin{pmatrix} (\mathbf{e}^i)' \\ (\tilde{\mathbf{e}}^i)' \end{pmatrix} &= 0 \\ B\,(\mathbf{e}^i)' + (\tilde{\mathbf{e}}^i)' &= 0 \end{aligned}$$

Therefore $(\tilde{\mathbf{e}}^i)'$ matches the i^{th} column of B, or equivalently $\tilde{\mathbf{e}}^i$ matches the i^{th} row of B'. Then the i^{th} row of A is identical to the i^{th} column of B. And this is true for all $1 \le i \le b$, so we have $B = A'$ and therefore $H_1 = H$. Hence, to a given G there corresponds a unique $H = (\, A' \quad I_{n-b}\,)$. Similar argument also holds if we start with a parity check matrix H given. ¶

Definition 11. Let C be a (b, n) code obtained from the generator matrix

$$G = [I_b \, A]$$

Then an $(n - b, n)$ matrix code defined by the parity check matrix

$$H = [A \, I_b]$$

is called the *dual code* $C^\perp$ of C.

Definition 12. Two words x and y are said to be in the same coset if and only if $y = x + c$ for some code word c in C.

Theorem 8. Two words x and y in $\mathbf{B}^n$ are in the same coset of C if and only if they have the same syndrome.

Proof. By Definition 12 x and y are in the same coset if and ony if

$$y = x + c$$

for some c in C, which in turn is true if and only if $x + y = c$ in C. Then it follows from this that,

$$\begin{aligned} H(\mathbf{x}+\mathbf{y})' &= 0 \\ H\left(\mathbf{x}'+\mathbf{y}'\right) &= 0 \\ H\mathbf{x}' + H\mathbf{y}' &= 0 \\ H\mathbf{x}' &= H\mathbf{y}' \end{aligned}$$

¶

Definition 13. Let F be a field. Then a non-empty set V is called a *vector space* over F if V and an addition form an Abelian group; for every a in F and v in V there is a uniquely defined element av in V such that for any v, v_1 and v_2 in V and any a and b in F,

$$a\left(v_1+v_2\right)=av_1+av_2$$

$$(a+b)v=av+bv$$

$$(ab)v=a(bv)$$

and

$$1v=v$$

1 being the identity of F.

Definition 14. Let V be a vector space over a field F. Then a set $\{v_1, \ldots, v_n\}$ of elements v_i in V is said to be *linearly independent* if

$$a_1 v_1 + \cdots + a_n v_n = 0$$

for $a_1, \ldots, a_n$ in F implies $a_1 = \cdots = a_n = 0$. A set $\{v_1, \ldots, v_n\}$ is called a *basis* of V if all its elements $v_1, \ldots, v_n$ in V are linearly independent over F and all elements in V may be expressed in the form $a_1 v_1 + \cdots + a_n v_n$ where all a_i, $i = 1, \ldots, n$, are in F. Also V is said to be of *dimension* n over F, $\dim V = n$. A map $f : V \to W$ from one vector space to another, where V and W are vector spaces over the same field F, is called an *isomorphism* if the map f one to one and onto and, for all v, v_1 and v_2 in V and a in F,

$$f\left(v_1 + v_2\right) = f\left(v_1\right) + f\left(v_2\right)$$

and

$$f(av) = af(v)$$

Theorem 9. Let two vector spaces V and W over the same field F have the same finite dimension. Then V and W are isomorphic.

Proof. Let $\dim V = \dim W = n$. Let $\{x_1, \ldots, x_n\}$ be a basis of V over F, and $\{y_1, \ldots, y_n\}$ a basis of W over F.

Since all the elements of V can be uniquely written as $a_1x_1 + \cdots + a_nx_n$ for some a_i in F, the map $f : V \to W$, which is

$$f\left(a_1x_1 + \cdots + a_nx_n\right) = a_1y_1 + \cdots + a_ny_n$$

for a_i in F, is well defined. Thus f is a homomorphism.

Since $f\left(a_1x_1 + \cdots + a_nx_n\right)$ implies $a_1y_1 + \cdots + a_ny_n = 0$ implies $a_1 = \cdots = a_n = 0$, which in turn implies $a_1x_1 + \cdots + a_nx_n = 0$, therefore f is one to one. Then, since all elements of W is of the form $a_1y_1 + \cdots + a_ny_n$, which is equal to $f\left(a_1x_1 + \cdots + a_nx_n\right)$ for some $a_1, \ldots, a_n$ in F, therefore f is also onto. Hence f is an isomorphism. ¶

Definition 15. Let

$$g(x) = g_0 + \cdots + g_k x^k$$

be a polynomial in $F[x]$. We call the *polynomial code* with encoding or generating polynomial $g(x)$ a code which encodes each original word of the message $a = (a_0, \ldots, a_{b-1})$, corresponding to

$$a(x) = a_0 + \cdots + a_{b-1}x^{b-1}$$

into the code word $b = (b_0, \ldots, b_{b+k-1})$, which corresponds to the code polynomial

$$b(x) = b_0 + \cdots + b_{b+k-1}x^{b+k-1} = a(x)g(x)$$

Note 1. We assume for our generating polynomial that $g_0 \neq 0$ and $g_k \neq 0$. To justify this assumption, suppose we have

$$g(x) = g_0 + \cdots + g_k x^k$$

If $g_0 = 0$, then we choose a new polynomial for$g(x)$ as

$$g_1(x) = a_1 + \cdots + a_k x^{k-1}$$

If $g_k = 0$, then we choose another polynomial

$$g_2(x) = g_0 + \cdots + a_{k-1} x^{k-1}$$

In either case our choice becomes more economical.

Theorem 10. A polynomial with coefficients in $\mathbf{B}$ is divisible by $1+x$ if and only if it has an even number of terms.

Proof. Let $f(x) = a_0 + \cdots + a_n x^n$ for all a_i in $\mathbf{B}$, $i = 1, \ldots, n$, and let $1+x|f(x)$. Then there exists a polynomial $b(x)$ in $\mathbf{B}$ such that

$$f(x) \equiv (1+x)b(x)$$

If $x = 1$, we have $a_0 + \cdots + a_n = 0$. Since the field $\mathbf{B}$ is of characteristic 2, this is only possible if the number of non-zero terms is even.

Conversely, let $f(x)$ have an even number of non-zero terms, say $f(x) = x^{i_1} + \cdots + x^{i_{2k}}$, where $i_1 < \cdots < i_{2k}$. Rewrite this as

$$f(x) = \left(x^{i_1} + x^{i_2}\right) + \cdots + \left(x^{i_{2k-1}} + x^{i_{2k}}\right)$$

For $i < j$, $x^i + x^j = x^i\left(1 + x^{j-i}\right) = x^i\left(1+x\right)\left(1 + \cdots + x^{j-i-1}\right)$, which means that $1 + x|x^i + x^j$. Therefore $1+x$ divides all bracketed terms in $f(x)$, and hence $1 + x|f(x)$. ¶

Theorem 11. If $g(x) \in \mathbf{B}[x]$ divides no polynomials of the form $x^k - 1$ for $k < n$, then the binary polynomial code of length n generated by $g(x)$ has the minimum distance of at least 3.

Proof. Let $g(x) = g_0 + \cdots + g_r x^r$, where g_i are in $\mathbf{B}$, $g_0 \neq 0$ and $g_r \neq 0$. Let $b = n - r$. Suppose the opposite to what the theorem says is true. Then, polynomial code being a group code, there exists $b(x)$ with at most two non-zero entries. There are two cases to consider, namely $b(x) = x^i + x^j$, where $i < j$, and $b(x) = x^i$, where $i < n$. In the first one of these, since n is the code length, we have $j < n$, hence $0 < j - i < n$. Since $g(x)|b(x)$ implies $g(x)|x^j\,(1 + x^{j-i})$, and $g_0 \neq 0$ implies $x \not| g(x)$, therefore $g(x)|1 + x^{j-i}$ which contradicts our hypothesis. In the second case, similarly to the above $g(x)|x^i$ and we again have a contradiction. ¶

Definition 16. Let C be a (b, n)-code. If there exists a $b \times n$ matrix G of rank b such that

$$C = \{\mathbf{a}G | a \in \mathbf{B}^b\}$$

then G is called a *generator matrix* of the code C, and C is called a *matrix code* generated by G.

Definition 17. Let C be a (b, n)-code. If there exists an $(n - b) \times n$ matrix H of rank $n - b$ such that

$$H\mathbf{b}' = 0$$

for all **b** in C, then H is called a *parity check matrix* of C.

Theorem 12. A polynomial code is a matrix code.

Proof. Let C be a polynomial b, n-code with the encoding polynomial $g(x) = g_0 + \cdots + g_k x^k$. Then $n = b + k$. Let G be the $b \times n$ matrix whose first row begins with entries $g_0, \ldots, g_k$ followed by b zeros, and whose succeeding row is an anticlockwise cyclic shift of the previous one, that is

$$G = \begin{bmatrix} g_0 & g_1 & \cdots & g_k & 0 & \cdots & 0 \\ 0 & g_0 & & \cdots & g_k & & \\ \vdots & & & & & & \\ 0 & & \cdots & & g_0 & \cdots & g_k \end{bmatrix}$$

The determinant of the submatrix formed by the first b columns is non-zero, since $g_0 \neq 0$ and hence $g_0^b \neq 0$. Thus the rank of G is m. Let the original word to be coded be $a = (a_0, \ldots, a_{m-1})$. Then, since the code word generated by aG is the same as that generated from $a(x)g(x)$, the two codes are identical. ¶

Algorithm 2 *Hamming codes*

```
**choose** $r$ a positive integer
$b \leftarrow 2^r - r - 1$
$n \leftarrow 2^r - 1$
**for** $i = 1$ to $2^r - 1$ **do**
    (the $i^{\text{th}}$ row of $M$)$\leftarrow (\mathbf{b}_i)$
**endfor**
**for** $i = 1$ to $2^r - 1$ **do**
    $(a_1, \ldots, a_{2^r-1}) \leftarrow (\mathbf{b}_i)$
    $(b_{2^{2-1}}, \ldots, b_{2^{r-2}} - 1, b_{2^{r-2}} + 1, \ldots, b_{2^{r-1}} - 1) \leftarrow (a_1, \ldots, a_{2^r-1})$
$(b_{2^{j-1}}; j = 1, \ldots, r) \leftarrow$ **solve** $(\mathbf{b}M = 0)$
the $i^{\text{th}}$ code word $\leftarrow (b_1, \ldots, b_n)$
**endfor**
```

Note 2. Each code word in a Hamming code contains

$$b - n = 2^r - r - 1 - 2^r + 1 = r$$

check digits. The value of r is called the

redundancy

of the code.